Full Privacy Policy

Contents

1. Introduction

Your privacy is important to Oyster Research Solutions Ltd (Oyster Research). When you choose to provide us with information about yourself, we recognise that you trust us to act in a responsible manner. So we've developed a Privacy Policy that covers how we collect, use, disclose, transfer, and store your information.

At all times, we will take all reasonable steps to ensure that your data is treated securely and in accordance with this privacy policy. By providing us with your information you consent to our use of it in the manner set out in this policy. Within the Privacy Policy you will find some specific examples of why and how we use your personal information. If you have further questions please get in touch with us by writing to Karin@oyster-research.com. Further information about us is available at the end of this document.

Please note: This Privacy Policy is available on our website. It's also available in hard copy upon request. In the event where you click on, or follow, any links from our site to external websites, our privacy policy will no longer apply. Please check the privacy policies of any such external site before submitting any personal data, as we cannot accept any responsibility or liability in relation to them.

2. What We Collect and Why

We will only use your personal information when we have a reason to use it. This might be because:

- you gave us consent to be in touch with you
- we have business dealings with you, e.g. a contract, or for instance sending project details if you have agreed to take part in one of our projects, or if you are a current or prospective client, or if you contact us with an enquiry and we use your contact details to respond
- we have to collect the information to fulfil a legal or regulatory obligation e.g. processing payroll information to pay our employees or suppliers
- we believe we, as a data controller o a third party (joint controller), have a legitimate business interest in using your personal information, e.g. showing a project film to a video editor when we want to explain what sort of footage we want them to produce for another project. The exception is where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

In addition, we may occasionally need to process personal information according to the following lawful grounds:

- to protect the vital interests of the data subject or of another natural person
- to perform a task carried out in the public interest or in the exercise of official authority vested in us as the data controller

We aim to be open about the way we use your personal information at the point we collect it, so we will always tell you why we need the information and what we will use the information for. Here are the ways we would intend to use your personal data and the legal basis for the processing.

Reason for Collection	Type of personal information	Legal Basis
Marketing communications and business updates	Name, Email address, Phone number	Consent or Legitimate interests
Respondent research project incentive payments	Name, Address, Bank details	Contract
Accounting	Name, Address, Email address , Phone number, Bank details, PO Number	Contract
New Client	Name, Email address , Postal address, Phone number, Payment type, PO Number	Contract

If you contact us by any channel with an enquiry, we will use the contact details you provided to respond to your enquiry and retain your contact details, as well as any additional personal information you may have given us as part of your enquiry, until such as time as we are satisfied that your enquiry has been fully addressed to your satisfaction.

If there is no ongoing relationship between us and you, your contact details and any other information you provided will then be deleted as outlined in our Data Protection Policy.

If there is an ongoing relationship between us and you, for instance because you are a customer, employee or contractor of Oyster Research, we will retain your details for as long as that relationship is necessary and for a number of years after the relationship is deemed to have ended as outlined in our Data Protection Policy

We may process your personal data for more than one purpose and therefore there may be more than one legal basis in use. If you would like more detail about how we use your personal information please email us at Karin@oyster-research.com and we will be happy to respond.

3. Information Collected from our Website

We do not directly collect any information about you when you visit www.oyster-research.com or www.oyster-research.co.uk, and our website does not hold contact forms so it does not collect information in this way about you.

Our website hosting provider may collect your IP address, details of which version of web browser you use as well as information on how you use the site, by using cookies. Cookies are small data files that are placed onto the hardware device which you use to browse the internet by websites that you visit. Please refer to our Cookie Policy for further information on the session cookies we use.

4. Information Collected from via Email / Verbally

We will also collect certain information if you contact us by email or if we speak by phone or in person.

What we collect:

- questions, queries or feedback you insert in the body of your email if you write to us or that you mention verbally. If you email us directly or via Karin@oyster-research.com we will also collect your email address

Why we collect it

- to provide you with information, products or services that you request from us or which we feel may interest you, where you have consented to be contacted for such purposes
- to carry out our obligations arising from any contracts entered into between you and us
- and, to notify you about changes to our service

- to gather feedback to improve our services
- respond to any feedback you send us

This information can be viewed by authorised people at Oyster Research and by our provider of IT/web services, Computrix Ltd.

5. Marketing Communications

We may send you or call you about marketing communications if you have:

- requested information about our products or services or made a purchase from us
- provided us with your information and requested that we send you marketing communications
- not opted out of receiving further marketing from us

We do not share your personal information with any other company for marketing purposes.
If at any time you want to stop receiving any marketing information you can email us at Karin@oyster-research.com and we will remove you from the marketing list. If you opt out of receiving any marketing communications, this will not apply to any communications related to the purchase of a product or service from us.

Please note we do not send out marketing alerts, newsletters or email campaigns for marketing purposes. We do not use a mail marketing package.

5. Research Project Information

As well as collecting personal information in the form of contact details in the normal course of business, as well as information for our research projects that may include personal participant information.

In the course of our research projects we may collect personal information from participants such as but not limited to their name, address, telephone number, job title, age, household information, and also on occasion their image. Occasionally we may carry out projects with children: here we take careful steps to ensure the information we provide young participants is accessible and appropriate for their age, and comply with local regulations or guidance in place governing parental consent.

Wherever possible, we put steps in place to anonymise your data at source: for instance using your first name only, and not linking comments you made during the course of the research to you. With large-scale quantitative surveys, we pseudonymise your data as a matter of course.

6. Sensitive Data

Sensitive data refers to data that includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data.

We do not routinely collect any sensitive data about you. However, from time to time we may need to collect some or all of the above sensitive data about you in order to fulfil the obligations of a designated research project we are working on. In this case we require your explicit consent for processing sensitive data and we will request your signature for this consent.

7. Keeping Your Personal Information Safe

To ensure the security of your personal data, we have put in place various security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

A summary of the steps we take to keep your information secure is outlined in this section. This is detailed further in our Data Protection Policy, available on request.

- We limit access to personal information to those employees, agents, contractors and third parties who require access in order to be able to perform a required service. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

- We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

- We use a range of technical and organisational measures to safeguard access to and use of, your personal information. These include hardware encryption and password protection, file encryption and password protection, anti-virus and anti-malware software deployment, physical access controls as outlined in our IT Security Policy, available on request.

8. Where your Personal Information is Stored

We store your information, whenever possible, on secure servers in the European Economic Area (EEA). Where it is necessary to disclose is to our processors or to joint controllers located outside the EEA, other jurisdictions which are acceptable according to guidance provided by the UK's Information Commissioner and/or where appropriate legal and security safeguards are in place, as determined by the UK authorities or the European Commission.

9. Data Retention

We will only retain your personal data for as long as necessary and to meet the need for which it was collected, including any legal, accounting and reporting requirements.

We have in place a retention policy for personal data and in defining the retention period, we considered the amount, nature and sensitivity of the personal data held as well as the purposes it was collected for and the potential harm that could arise from the unauthorised access or disclosure of the information. Additionally any legal, regulatory or compliance requirements for the data to be held was also considered.

By law we have to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for seven years after they cease being customers for tax purposes.

In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

10. Disclosing your Personal Information

We may pass on your personal information if we have a legal obligation to do so, or if we have to enforce or apply our terms of use or other agreements we have in place. This may include disclosing to other companies and organisations in connection with fraud protection and credit risk reduction.

So, on occasion, we may have to share your personal information with third parties in order to meet our obligations or provide a service. These parties are set out below for your reference:

- Service providers who provide IT and system administration services
- Professional market research associates who may be assisting on projects
- Professional advisers including lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services
- HM Revenue & Customs, regulators and other authorities based in the United Kingdom and other relevant jurisdictions who require reporting of processing activities in certain circumstances

Before we transfer or share your information with any third parties we will make sure that they have in place processes and procedures to ensure the security of your information and to treat it in accordance with data protection legislation. We would only allow third parties access to your information for specified purposes and in accordance with our instructions.

We won't share your information with any other organisations for commercial purposes, and we don't pass on your details to other websites.

11. Transferring your Personal Information

During the course of a project, we may pass on your personal information to approved subcontractors acting as part of our team on our projects and subject to Data Processor Agreements and to other Oyster Research policies if required. The majority of our subcontractors are based in the UK and we do not routinely transfer your personal data outside the EEA.

For some projects, however, we may use sub-contractors based in other parts of the European Economic Area (EEA)* or in non-EEA countries part of the European Free Trade Area (EFTA)** or in assured territories*** that the EU Commission deems safe for the purpose of data protection or in the US covered by the EU-US Privacy Shield.

Whenever we transfer your personal data out of the EEA, we do our best to ensure a similar degree of security of data by ensuring at least one of the following safeguards is implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission or
- Where we use certain service providers, we may use specific contracts or codes of conduct or certification mechanisms approved by the European Commission which give personal data the same protection it has in Europe or
- Where we use providers based in the United States, we may transfer data to them if they are part of the EU-US Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US

If none of the above safeguards is available and the transfer of data is essential then we may request your explicit consent to the specific transfer.

** EEA countries include: Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom. **EFTA countries include: EEA countries plus Switzerland. ***Assured territories include: Andorra, Argentina, Canada, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Faroe Islands, Uruguay. The European Commission has agreed that these territories can provide adequate safeguards for the purposes of the Directive. Transfers out of the EEA and into these territories will not breach the adequate safeguard requirement. The list may also be subject to change from time to time as new adequacy rulings are made by the European Commission.*

12. Your Rights

You have a number of rights about how the personal information you provide can be used. These are:

- **The right to be informed**: transparency over how personal information is used
- **The right of access**: the ability to request a copy of the information held which will be provided within one month
- **The right to rectification**: update or amend the information we hold about you if it is wrong
- **The right to erasure/to be forgotten**: remove personal information from records
- **The right to restrict processing**: cease the use of the information
- **The right to data portability**: obtain and reuse personal information for your own purposes
- **The right to object**: object to the processing of information for marketing purposes
- **Rights in relation to automated decision making and profiling**: not be subject to a decision when it is based on automated processing

If you would like to know more about your rights under the data protection law, you can find out more at the Information Commissioners Office website. You can change the way you hear from us or withdraw your permission for us to processing your personal information at any time by sending us an email Karin@oyster-research.com

13. How to Contact Us

If you wish to talk through anything in our privacy policy, find out more about your rights or obtain a copy of the information we hold about you, please contact us by email or mail and we will be happy to help.

If you wish to raise a complaint on how we have handled your personal information, you can contact us and we will investigate the matter. If you are not satisfied with our response or believe we are not processing your personal information in accordance with the law you can complain to the Information Commissioner's Office (ICO).

To contact us, our email address is Karin@oyster-research.com
Or you can write to us at 12 Upavon Drive, Reading, RG1 6LP.

14. About Us

Oyster Research Solutions Ltd is a private limited company registered in England and Wales (Company Number 06196116). Registered address: 12 Upavon Drive, Reading, RG1 6LP

Full Privacy Policy
Version 1
Date of issue: May 2018